Protection des connexions unicast sous MPLS

Le développement de l'internet a été derrière le déploiement d'un nombre élevé d'applications temps réel comme la téléphonie IP, les jeux en réseau et la TV numérique. Ces applications ont des contraintes de temps qui doivent être vérifiées ; elles ont donc besoin de tourner sur des réseaux robustes et résistants aux pannes. Pour ce faire, différentes techniques de protection ont été élaborées. Ces dernières ont pour rôle de diminuer ou d'éviter les ruptures de connexion en configurant des chemins de secours permettant de recevoir et de router le trafic des connexions affectées par une panne.

Pour diminuer les délais de récupération des pannes (délai entre le moment où la panne est détectée et le moment où le trafic des connexions affectées par la panne est redirigé vers les connexions de secours), les techniques de protection locale et proactive sont utilisées. Avec de telles techniques, les chemins de secours sont établis à l'avance et avant toute panne. Lorsqu'une panne est détectée par un routeur, ce dernier bascule le trafic rapidement vers le(s) chemin(s) permettant de contourner la panne.

Avec l'arrivée de MPLS (Multi-Protocol Label Switching), les délais de récupération ont considérablement diminué (de l'ordre de 50 ms) grâce à :

1- Flexibilité dans le choix des chemins de secours,
2- Pré-établissement des chemins de secours et reroutage du trafic vers ces derniers rapidement.

Deux types de chemins (dits LSP) de secours existent sous MPLS : NHOP (Next HOP) et NNHOP (Next Next HOP). Le premier type de LSP de secours permet de protéger une connexion contre la panne d'un lien et le second la protège contre la panne d'un nœud. Le principe de construction est le même pour les deux types des LSP de secours : il s'agit de prédéterminer un chemin de secours pour chaque composant (lien ou routeur) du chemin primaire (transportant le trafic en l'absence de pannes) de la connexion permettant de le contourner et de pallier ainsi son éventuelle panne.

Dans ce projet, on propose d'utiliser des topologies de réseau générées aléatoirement avec l'approche de Waxman (topologies de réseau fournies) sur lesquelles il sera demandé dans un premier temps de déterminer les chemins primaires des connexions. Pour ce faire l'algorithme de Dijkstra sera utilisé. Ensuite, l'algorithme de Dijkstra sera modifié pour permettre le pré-établissement des chemins de secours permettant la protection, contre les pannes simples, des composants supportant les connexions primaires. Dans ce cadre, il sera demandé d'implémenter différentes approches pour le calcul des chemins de secours tenant compte du partage de la bande passante.

Environnement :

- C++,
- Bibliothèque LEDA : Cette bibliothèque comporte différentes fonctions permettant la gestion des graphes (topologies de réseau),
- Un compte à l'IRISA permettant d'accéder à la station de travail AFRIQUE qui sert de serveur à LEDA,
- Manuel d'utilisateur de LEDA,
- RFC 4090 intitulé : "Fast Reroute Extensions to RSVP-TE for LSP Tunnels".